(19)日本国特許庁(JP)　(12)公開特許公報（A）　(11)特許出願公開番号

特開平１０－１０７８３２

(43)公開日　平成10年(1998)4月24日

(51)Int. Cl.[6]		識別記号	FI		
H04L	12/54		H04L	11/20	１０１　B
	12/58		G06F	13/00	３５１　G
G06F	13/00	３５１	G09C	1/00	６６０　G
G09C	1/00	６６０	H04L	9/00	６４１
H04L	9/14			11/18	

審査請求　未請求　請求項の数５　ＯＬ　（全１０頁）　最終頁に続く

(21)出願番号　特願平8-253599

(22)出願日　平成8年(1996)9月25日

(71)出願人　000233055
日立ソフトウエアエンジニアリング株式会社
神奈川県横浜市中区尾上町6丁目81番地

(72)発明者　鮫島　吉喜
神奈川県横浜市中区尾上町6丁目81番地
日立ソフトウェアエンジニアリング株式会社内

(74)代理人　弁理士　秋田　収喜

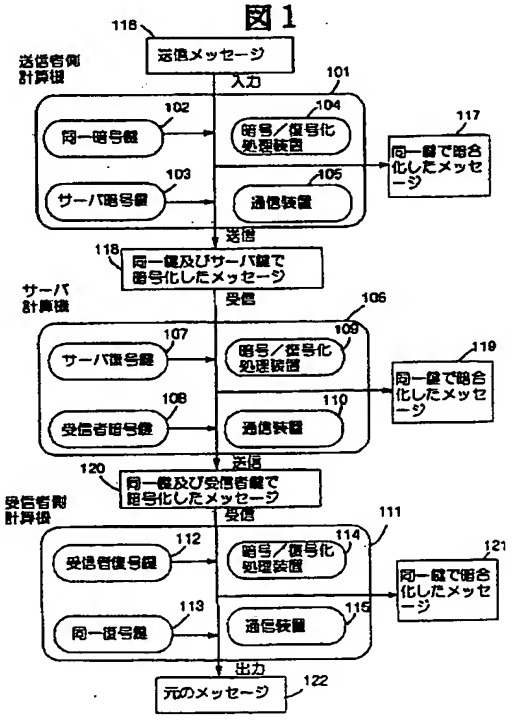
(54)【発明の名称】暗号同報メールシステム

(57)【要約】

【課題】　正規のメンバであった者がメーリングリストメンバから抜けた後に、メッセージを不法入手するのを防止し、セキュリティ上の向上を図る。

【解決手段】　送信者はメンバの持っている同一鍵で、メッセージを暗号化し、さらにメーリングリストサーバの鍵で暗号化して、サーバに送信する。サーバは受け取った鍵で復号し、次にメンバ（ここでは受信者を指す）各自が持っている復号鍵に対応する暗号鍵でそれぞれ暗号化し、メンバに送信する。２重に暗号化されたメッセージを受け取ったメンバである受信者は、まず、自分だけが持っている復号鍵で復号し、さらにメーリングリスト共通の復号鍵で復号する。

図1



1

【特許請求の範囲】

【請求項１】　通信網によって相互接続された複数の送受信者の計算機と同報メール機能を有するメールサーバ計算機からなる同報メールシステムにおいて、
送信者計算機が、メールの受信者計算機が記憶している復号鍵に対応する暗号鍵を用いてメッセージを暗号化した後、サーバ計算機だけもしくはサーバ計算機と送信者計算機のみが記憶している復号鍵に対応する暗号鍵でさらにメッセージを暗号して、メールサーバ計算機に送信し、メールサーバ計算機は、暗号鍵に対応する復号鍵で一度復号して、受信者計算機に送信することを特徴とする暗号同報メールシステム。

【請求項２】　請求項１記載の暗号同報メールシステムにおいて、メールサーバ計算機が一度復号した後、サーバ計算機だけもしくはサーバ計算機と各受信者計算機のみが記憶している復号鍵に対応する暗号鍵でメッセージを暗号して、各受信者計算機に送信することを特徴とする暗号同報メールシステム。

【請求項３】　請求項２記載の暗号同報メールシステムにおいて、メールの受信者計算機が記憶している復号鍵に対応する暗号鍵を用いてメッセージを直接暗号するのではなく、メッセージごとにメッセージ暗号鍵とメッセージ復号鍵を生成し、このメッセージ暗号鍵でメッセージを暗号し、メッセージ復号鍵をメールの受信者計算機が記憶している復号鍵に対応する暗号鍵を用いて暗号化することを特徴とする暗号同報メールシステム。

【請求項４】　請求項３記載の暗号同報メールシステムにおいて、送信者計算機がメールの受信者計算機が記憶している復号鍵に対応する暗号鍵を用いてメッセージ復号鍵を暗号した後、サーバ計算機だけもしくはサーバ計算機と送信者計算機のみが記憶している復号鍵に対応する暗号鍵でメッセージ復号鍵をさらに暗号して、暗号したメッセージとメッセージ復号鍵をメールサーバ計算機に送信し、メールサーバ計算機は、暗号鍵に対応する復号鍵で暗号したメッセージ復号鍵を一度復号して、暗号したメッセージとメッセージ復号鍵を受信者計算機に送信することを特徴とする暗号同報メールシステム。

【請求項５】　請求項４記載の暗号同報メールシステムにおいて、メールサーバ計算機が暗号したメッセージ復号鍵を一度復号した後、サーバ計算機だけもしくはサーバ計算機と各受信者計算機のみが記憶している復号鍵に対応する暗号鍵でメッセージ復号鍵を暗号して、各受信者計算機に暗号したメッセージとメッセージ復号鍵を送信することを特徴とする暗号同報メールシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、電子メールシステムの中にある同じ内容のメッセージを複数の人に同報送信する、いわゆる同報メールもしくはメーリングリストサービスに係わる暗号同報メールシステムに関する。

2

【０００２】

【従来の技術】メーリングリストで暗号機能を実現するには、従来、３つの方法が知られている。第１の方法は、メーリングリストのメンバに同一の復号鍵を配布し、この復号鍵に対応する暗号鍵を用いてメッセージを暗号化して送信する方法である。

【０００３】第２の方法は、それぞれのメンバが復号鍵を持ち、送信者がそれぞれのメンバ受信者の復号鍵に対応する暗号鍵を用いて暗号化して送る方法である。

【０００４】第３の方法は、それぞれのメンバが復号鍵を持ち、メーリングリストサーバメーリングリスト管理プログラムがそれぞれのメンバの復号鍵に対応する暗号鍵を用いて暗号化して送る方法である。

【０００５】

【発明が解決しようとする課題】前記従来技術には以下のような問題点が挙げられる。

【０００６】前記第１の方法には、メーリングリストメンバが減った場合に問題が起こる。つまり、正規のメンバであった者が、メーリングリストメンバから抜けた後に、ネットワークを盗聴するなどしてメッセージを不法入手し、持っている復号鍵を使って暗号化されたメッセージを復号することができてしまう。これを防ぐためには、メンバが減る度に全てのメンバの鍵を交換する必要がおきてしまい、時間およびコストがかかってしまう。

【０００７】第２の方法では、全ての送信者が全てのメンバの暗号鍵をもっている必要があることに問題がある。例えば、メンバの増減や鍵の交換があると、その度に全ての送信者が自分が保有するメンバの構成を更新したりメンバの鍵を更新する必要があり、第１の方法と同様にコストがかかる。

【０００８】第３の方法では、本来メンバには含まれないメーリングリストサーバが、そして結果的にはサーバの管理者がメッセージ本体にアクセスすることができ、セキュリティ上の問題が生じる。

【０００９】本発明の目的は、これらの問題を解決する暗号同報メールシステムを提供することである。

【００１０】

【課題を解決するための手段】本発明は、メーリングリストサーバを用い、メッセージを二重に暗号することで課題を解決する。暗号に用いる鍵として、メンバそれぞれの鍵、メーリングリストサーバの鍵、メンバ共通の鍵同一鍵を用いる。鍵には暗号に使う鍵と復号に使う鍵の２種類がある。公開鍵暗号方式では、暗号鍵と復号鍵は別の鍵であり、暗号鍵は送信者を含め誰でもアクセスでき公開鍵と呼ばれ、復号鍵は受信者のみアクセスでき個人鍵と呼ばれる。対称鍵暗号方式では、２つの鍵は同一であり秘密鍵と呼ばれることが多い。

【００１１】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態を詳細に説明する。

【００１２】図１は、本発明を適用したシステムの第１の実施形態を示すシステム構成図である。

【００１３】１０１はメーリングリストの参加メンバであり、メーリングリストにメッセージを送る送信者の計算機である。１０２は前記メーリングリストにメッセージを送る送信者の計算機１０１が記憶している、メーリングリストの全てのメンバの計算機が持っている同一暗号鍵である。

【００１４】１０３は、計算機１０１が記憶しており、メーリングリストの全てのメンバの計算機が持っているサーバの暗号鍵である。１０４は、計算機１０１が備えており、同一暗号鍵１０２、サーバ暗号鍵１０３の鍵を使ってメッセージの暗号処理や復号処理を行う暗号／復号装置である。１０５は、計算機１０１が備えており、メッセージをネットワークへ送信する通信装置である。

【００１５】１０６はメーリングリストのサーバ計算機である。１０７は、サーバ計算機１０６が記憶し、サーバ暗号鍵１０３に対応する復号鍵であり、サーバ計算機１０６だけが記憶している。１０８は、サーバ計算機１０６が記憶しており、メンバそれぞれの固有の暗号鍵である。なお、メンバの暗号鍵はメンバの数だけある。

【００１６】１０９はサーバ計算機１０６が備えており、サーバ復号鍵１０７、メンバ固有の暗号鍵１０８を使ってメッセージの暗号や復号を行う暗号／復号装置である。

【００１７】１１０はサーバ計算機１０６に備えられており、メッセージをネットワークから受信したり、ネットワークへ送信したりする通信装置である。１１１はメーリングリストの参加メンバであり、サーバ計算機から送られてきたメッセージを受け取る受信者の計算機である。

【００１８】１１２は受信者計算機１１１が記憶しており、メンバ固有の暗号鍵１１２に対応する復号鍵であり、受信者計算機１１１だけが記憶している。１１２は受信者計算機１１１が記憶しており、メーリングリストの全てのメンバが持っている同一暗号鍵１０２に対応する同一の復号鍵であり、メンバの計算機だけが記憶している。１１４は受信者計算機１１１が備えており、復号鍵１１２、同一復号鍵１１３の鍵を使ってメッセージの暗号や復号を行う暗号／復号装置である。

【００１９】１１４は受信者計算機１１１が備えており、メッセージをネットワークから受信する装置である。１１６は送信者が作成するメッセージを示す。１１７は送信者計算機の中で同一暗号鍵１０２と暗号／復号装置１０４を使ってメッセージ１１６を暗号化したメッセージである。

【００２０】１１８はサーバ暗号鍵１０３と暗／復号装置１０４を使って暗号メッセージ１１７をさらに暗号化したメッセージであり、送信者計算機からサーバ計算機へ通信装置１０５を使いネットワークを経由して送信される。１１８は同一暗号鍵１０２とサーバ暗号鍵１０３の鍵を使い、二重に暗号化されている複合暗号メッセージである。

【００２１】１１９はサーバ計算機の中でサーバ復号鍵１０７と暗号／復号装置１０９を使って暗号メッセージ１１８を復号化したメッセージであり、暗号メッセージ１１７と同一である。

【００２２】１２０はメンバ固有の暗号鍵１０８と暗号/復号装置１０９を使って、暗号メッセージ１１９を暗号化したメッセージであり、サーバ計算機から受信者計算機へ通信装置１１０を使い、ネットワークを経由して送信される。

【００２３】１２１はサーバ計算機の中で復号鍵１１２と暗号／復号装置１１４を使って暗号メッセージ１２０を復号化したメッセージであり、暗号メッセージ１１７、１１９と同一である。１２２はサーバ計算機の中で同一復号鍵１１３と暗号／復号装置１１４を使って暗号メッセージ１２１を復号、出力したメッセージで、メッセージ１１６と同一である。なお、本明細書の実施の形態および、図面において、送信者側計算機と受信者側計算機はそれぞれ、単数で開示しているのは説明上の都合であり、それぞれが複数あっても構わない。

【００２４】以下、図２のフロー図にしたがって、具体的な処理を説明する。

【００２５】ステップ２０１からステップ２０４までは、送信者計算機１０１の処理を示す。ステップ２０５からステップ２０８までは、サーバ計算機１０６の処理を示す。ステップ２０９からステップ２１２までは、受信者計算機１１１の処理を示す。

【００２６】送信者がメーリングリスト宛のメッセージ１１６を作成し送信者計算機１０１に入力する（ステップ２０１）。送信者計算機１０１が同一暗号鍵１０２と暗号／復号装置１０４を用いて入力されたメッセージ１１６を暗号化し、同一鍵で暗号化したメッセージ１１７を生成する（ステップ２０２）。

【００２７】送信者計算機１０１がサーバ暗号鍵１０３と暗号/復号装置１０４を用いて、同一鍵で暗号したメッセージ１１７をさらに暗号化し、同一鍵およびサーバ鍵で暗号化したメッセージ１１８を生成する（ステップ２０３）。送信者計算機１０１が通信装置１０５を用いて、先に生成したメッセージ１１８をサーバ計算機１０６宛にネットワークを経由して送信する（ステップ２０４）。

【００２８】送信者計算機１０１が送信した暗号メッセージ１１８をサーバ計算機１０６が、通信装置１１０を用いて受信する（ステップ２０５）。サーバ計算機１０６がサーバ復号鍵１０７と暗号/復号装置１０９を用いて受信したメッセージ１１８を復号し、同一鍵で暗号化したメッセージ１１９を生成する（ステップ２０６）。

【００２９】サーバ計算機１０６が、受信者暗号鍵１０

８と暗号/復号装置１０９を用いて同一鍵で暗号したメッセージ１１９を暗号化し、同一鍵および受信者鍵で暗号したメッセージ１２０を生成する（ステップ２０７）。

【００３０】このステップ２０７の処理は受信者であるメーリングリストのメンバそれぞれに対して行う。つまり、それぞれの受信者の暗号鍵で暗号化し、各受信者ごとに暗号メッセージ１２０を生成する。

【００３１】サーバ計算機１０６が通信装置１１０を用いて、先に生成したメッセージ１２０を受信者計算機１１１宛にネットワークを経由して、送信する（ステップ２０８）。このステップ２０８の処理もそれぞれの受信者に対して繰り返す。つまり、それぞれの受信者の計算機に対応するメッセージ１２０を送信する。

【００３２】サーバ計算機１０６が送信した暗号メッセージ１２０を受信者計算機１１１が、通信装置１１５を用いて受信する（ステップ２０９）。受信者計算機１１１が受信者復号鍵１１２と暗号/復号装置１１４を用いて受信したメッセージ１２０を復号し、同一鍵で暗号したメッセージ１２１を生成する（ステップ２１０）。

【００３３】受信者計算機１１１が同一復号鍵１１３と暗号/復号装置１１４を用いて同一鍵で暗号したメッセージ１２１を復号する（ステップ２１１）。そして、この復号したメッセージ１１２を受信者に対して、出力する（ステップ２１２）。

【００３４】（実施の形態２）次に、図３、図４を用いて本発明の第２の実施形態を詳細に説明する。

【００３５】図３は全体のシステム構成を示す。図３において、３０１はメーリングリストの参加メンバであり、メーリングリストにメッセージを送る送信者の計算機である。３０２は送信者計算機３０１が記憶しており、メーリングリストの全てのメンバの計算機が持っている同一の暗号鍵である。

【００３６】３０３は送信者計算機３０１が記憶しており、メーリングリストの全てのメンバの計算機が持っているサーバの暗号鍵である。３０４は送信者計算機３０１が備えており、メッセージ鍵の生成及びメッセージ鍵３０２、３０３の鍵を使ってメッセージやメッセージ復号鍵の暗号や復号を行う装置である。３０５は送信者計算機３０１が備えており、メッセージや鍵をネットワークへ送信する装置である。

【００３７】３０６はメーリングリストのサーバ計算機である。３０７はサーバ計算機３０６が記憶しており、サーバ暗号鍵３０３の暗号鍵に対応する復号鍵であり、サーバ計算機３０６の計算機だけが記憶している。３０８は、サーバ計算機３０６が記憶しており、メンバそれぞれの暗号鍵である。メンバの暗号鍵はメンバの数だけある。３０９は、サーバ計算機３０６が備えており、サーバ復号鍵３０７、受信者暗号鍵３０８の鍵を使ってメッセージやメッセージ復号鍵の暗号や復号を行う装置である。３１０は、サーバ計算機３０６が備えており、メッセージや鍵をネットワークから受信したり、ネットワークへ送信する装置である。

【００３８】３１１はメーリングリストの参加メンバであり、サーバ計算機から送られてきたメッセージを受け取る受信者の計算機である。３１２は受信者計算機３１１が記憶しており、受信者暗号鍵３０８に対応する復号鍵であり、受信者計算機３１１だけが記憶している。

【００３９】鍵作成／暗号化／復号化処理装置３０４は受信者計算機３１１が記憶しており、メーリングリストの全てのメンバが持っている同一暗号鍵３０２に対応する同一の復号鍵であり、メンバの計算機だけが記憶している。

【００４０】３１４は受信者計算機３１１が備えており、受信者復号鍵３１２、鍵作成/暗号化／復号化処理装置３０４を使ってメッセージやメッセージ復号鍵の暗号や復号を行う装置である。

【００４１】３１５は、受信者計算機３１１が備えており、メッセージや鍵をネットワークから受信する装置である。３１６は送信者が作成するメッセージを示す。３１７は鍵作成／暗号化／復号化処理装置３０４が生成したメッセージ復号鍵である。

【００４２】３１８は発信者計算機の中で鍵作成／暗号化／復号化処理装置３０４が生成したメッセージ暗号鍵と鍵作成／暗号化／復号化処理装置３０４を使って送信メッセージ３１６を暗号化したメッセージである。３１９は同一暗号鍵３０２と鍵作成／暗号化／復号化処理装置３０４を使ってメッセージ復号鍵３１７を暗号化されたメッセージ復号鍵である。

【００４３】３２０は暗号メッセージ３１８と同一であり、送信者計算機３０１からサーバ計算機３０６へ通信装置３０５を使い、ネットワークを経由して送信される。３２１はサーバ暗号鍵３０３と鍵作成／暗号化／復号化処理装置３０４を使って、メッセージ復号鍵３１９を暗号したメッセージ復号鍵であり、送信者計算機３０１からサーバ計算機３０６へ通信装置３０５を使い、ネットワークを経由して送信される。

【００４４】メッセージ復号鍵３２１は同一暗号鍵３０２とサーバ暗号鍵３０３の鍵を使い、二重に暗号化されている。暗号化メッセージ３２２は暗号化メッセージ３１８、３２０と同一で受信した暗号メッセージである。３２３はサーバ計算機の中でサーバ復号鍵３０７と暗号復号化装置３０９を使って、メッセージ復号鍵３２１を復号したメッセージ復号鍵である。

【００４５】３２４は暗号化メッセージ３１８、３２０、３２２と同一であり、サーバ計算機３０６から受信者計算機３１１通信装置３１０を使い、ネットワークを経由して送信される。

【００４６】３２５は受信者暗号鍵３０８と暗号復号装置３０９を使って、メッセージ復号鍵３２３を暗号化し

たメッセージ復号鍵であり、サーバ計算機３０６から受信者計算機３１１へ通信装置３１０を使い、ネットワークを経由して送信される。

【００４７】３２６は暗号化メッセージ３１８、３２０、３２２、３２２と同一であり、受信した暗号メッセージである。３２６はサーバ計算機の中で受信者復号鍵３１２と暗号復号装置３１４を使ってメッセージ復号鍵３２５を復号したメッセージ復号鍵である。

【００４８】３２８は同一復号鍵３１３と暗号復号装置３１４を使って、メッセージ復号鍵３２７を復号したメッセージ復号鍵で、メッセージ復号鍵３１７と同一である。

【００４９】３３０はサーバ計算機の中でメッセージ復号鍵３２８と暗号復号装置３１４を使って、暗号化メッセージ３２６を復号、出力したメッセージで、送信メッセージ３１６と同一である。

【００５０】以下、図４のフロー図にしたがって、処理を説明する。

【００５１】ステップ４０１から４０６までは、送信者計算機３０１の処理を示す。ステップ４０７から４１０までは、サーバ計算機３０６の処理を示す。ステップ４１１から４１５までは、受信者計算機３１１の処理を示す。

【００５２】送信者がメーリングリスト宛のメッセージ３１６を作成し、送信者計算機３０１に入力する（ステップ４０１）。送信者計算機３０１が鍵生成／暗復号装置３０４を使ってメッセージ暗号鍵とメッセージ復号鍵３１７を生成する（ステップ４０２）。

【００５３】送信者計算機３０１が先に生成したメッセージ暗号鍵と鍵生成/暗復号装置３０４を用いて入力された送信メッセージ３１６を暗号化し、メッセージ鍵で暗号したメッセージ３１８を生成する（ステップ４０３）。

【００５４】送信者計算機３０１が同一暗号鍵３０２と鍵作成／暗号化／復号化処理装置３０４を用いてメッセージ復号鍵３１７を暗号化し、同一鍵で暗号したメッセージ復号鍵３１９を生成する（ステップ４０４）。

【００５５】送信者計算機３０１がサーバ暗号鍵３０３と鍵作成／暗号化／復号化処理装置３０４を用いて同一鍵で暗号化したメッセージ復号鍵３１９をさらに暗号化し、同一鍵およびサーバ鍵で暗号したメッセージ復号鍵３２１を生成する（ステップ４０５）。

【００５６】送信者計算機３０１が通信装置３０５を用いて、先に暗号したメッセージ３１８、３２０と同一と同一鍵およびサーバ鍵で暗号したメッセージ復号鍵３２１をサーバ計算機３０６宛にネットワークを経由して送信する（ステップ４０６）。

【００５７】送信者計算機３０１が送信したメッセージ３２０とメッセージ復号鍵３２１をサーバ計算機サーバ計算機３０６が通信装置３１０を用いて、受信する（ステップ４０７）。

【００５８】サーバ計算機３０６がサーバ復号鍵３０７と暗号／復号装置３０９を用いて、受信したメッセージ復号鍵３２１を復号し、同一鍵で暗号したメッセージ復号鍵３２３を生成する（ステップ４０８）。この時、暗号したメッセージ３２２はそのままである。

【００５９】サーバ計算機３０６が、受信者暗号鍵３０８と暗号／復号装置３０９を用いて同一鍵で暗号したメッセージ復号鍵３２３を暗号化し、同一鍵および受信者鍵で暗号化したメッセージ復号鍵３２５を生成する（ステップ４０９）。このステップ４０９の処理は、受信者であるメーリングリストのメンバそれぞれに対して行う。つまり、それぞれの受信者の暗号鍵で暗号し、各受信者ごとに暗号したメッセージ復号鍵３２５を生成する。

【００６０】サーバ計算機３０６が通信装置３１０を用いて、先に生成したメッセージ復号鍵３２５と暗号したメッセージ（３２２、３２４と同一）を受信者計算機３１１宛にネットワークを経由して送信する（ステップ４１０）。このステップ４１０の処理もそれぞれの受信者に対して繰り返す。つまり、それぞれの受信者の計算機に暗号したメッセージ３２４と受信者に対応するメッセージ復号鍵３２５を送信する。

【００６１】サーバ計算機３０６が送信した暗号したメッセージ３２４とメッセージ復号鍵３２５を受信者計算機３１１が通信装置３１５を用いて受信する（ステップ４１１）。

【００６２】受信者計算機３１１が受信者復号鍵３１２と暗号／復号装置３１４を用いて受信したメッセージ復号鍵３４９を復号し、同一鍵で暗号したメッセージ復号鍵３２７を生成する（ステップ４１２）。この時、暗号したメッセージ３２６はそのままである。

【００６３】受信者計算機３１１が受信者復号鍵３１２と暗号／復号装置３１４を用いて同一鍵で暗号したメッセージ復号鍵３２７を復号し、元のメッセージ復号鍵３１７と同じメッセージ復号鍵３２８を得る（ステップ４１３）。暗号化したメッセージ３２６３をメッセージ復号鍵３２８と暗号／復号装置３１５を用いて復号する（ステップ４１４）。この復号したメッセージ３３０を受信者に対して出力する（ステップ４１５）。

【００６４】

【発明の効果】本発明によると、送信者からサーバに送られるメッセージもしくはメッセージ復号鍵は、メンバが共通に持っている鍵で暗号され、さらにサーバの鍵で暗号されているので、サーバだけが復号できる。

【００６５】また、メーリングリストから抜けてしまったメンバはたとえ、メンバ同一の復号鍵を持っていてもアクセスできない。メンバが減った時には、メールサーバ計算機内部の変更だけで済み、メンバ送受信者の計算機の変更が不要になる。

9

【００６６】また、メッセージもしくはメッセージ復号鍵はメンバ計算機だけが復号できる同一鍵で暗号されているのでメールサーバ計算機はアクセスすることができす、第３者による盗聴、情報の漏洩を防ぐことができる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態を示すシステム構成図である。

【図２】本発明の第１の施の形態の処理を示すフローチャートである。

10

【図３】本発明の第２の実施形態を示すシステム構成図である。

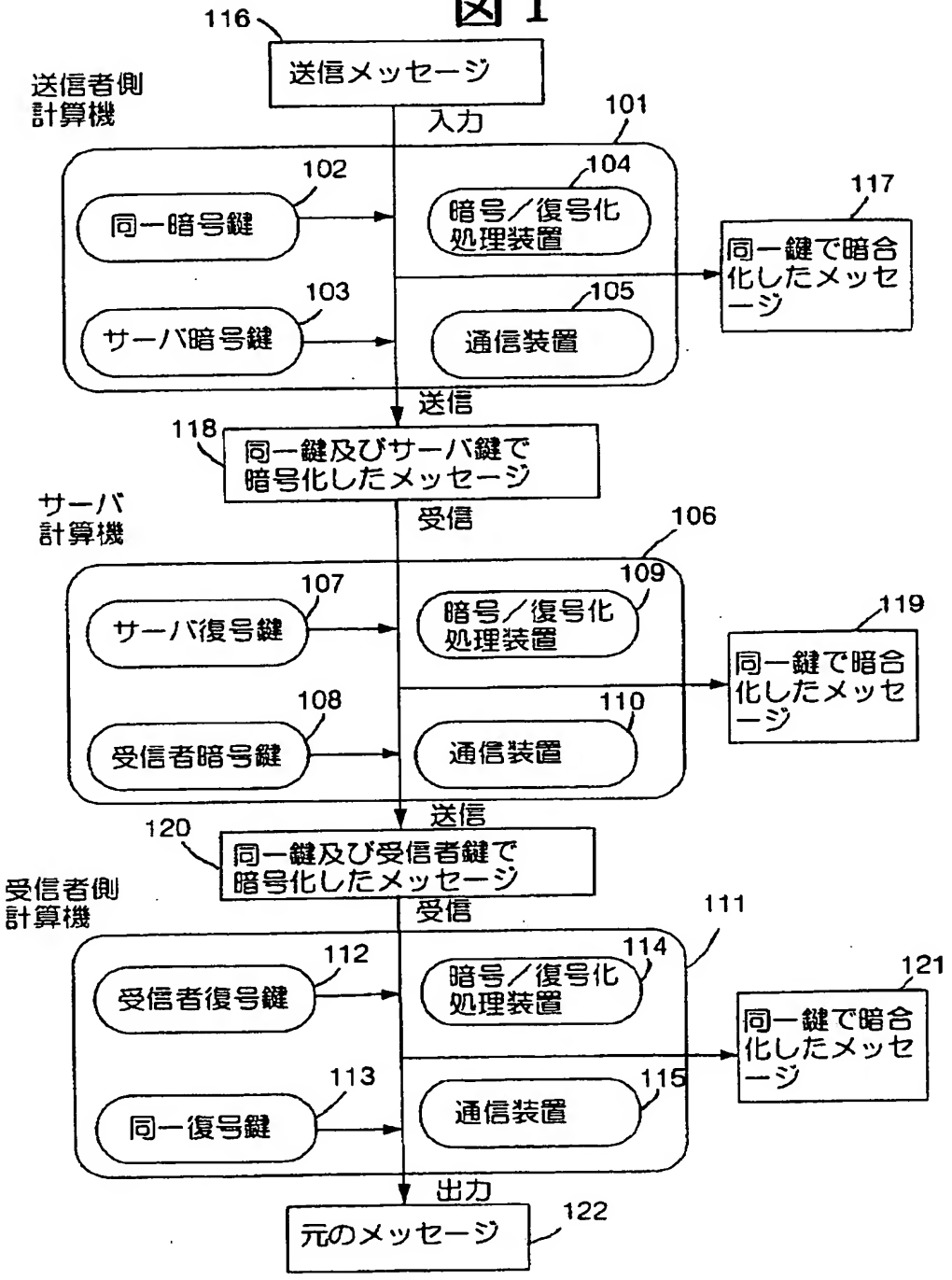
【図４】本発明の第２の実施の形態の処理を示すフローチャートである。

【符号の説明】

１０２…同一暗号鍵、１０３…サーバ暗号鍵、１０４，１０９，１１４…暗号/復号化処理装置、１０５，１１０，１１５…通信装置、１０７…サーバ復号鍵、１０８…受信者暗号鍵、１１２…受信者復号鍵、１１３…同一復号鍵。

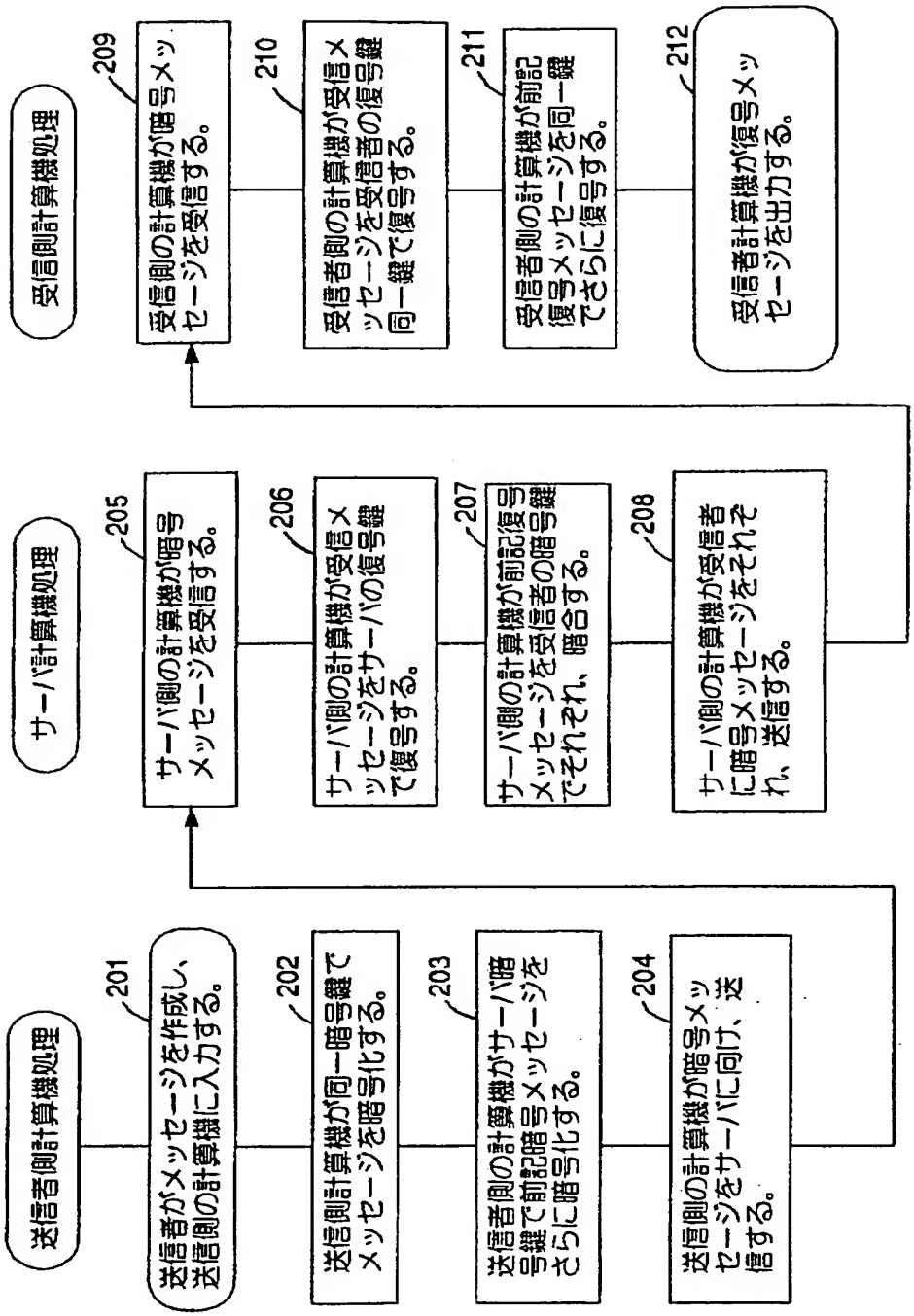
【図１】

図 1


116
送信メッセージ
送信者側
計算機
入力
101
102
同一暗号鍵
104
暗号／復号化
処理装置
117
同一鍵で暗合
化したメッセ
ージ
103
サーバ暗号鍵
105
通信装置
送信
118
同一鍵及びサーバ鍵で
暗号化したメッセージ
サーバ
計算機
受信
106
109
107
サーバ復号鍵
暗号／復号化
処理装置
119
同一鍵で暗合
化したメッセ
ージ
108
受信者暗号鍵
110
通信装置
送信
120
同一鍵及び受信者鍵で
暗号化したメッセージ
受信者側
計算機
受信
111
112
受信者復号鍵
114
暗号／復号化
処理装置
121
同一鍵で暗合
化したメッセ
ージ
113
同一復号鍵
115
通信装置
出力
元のメッセージ
122

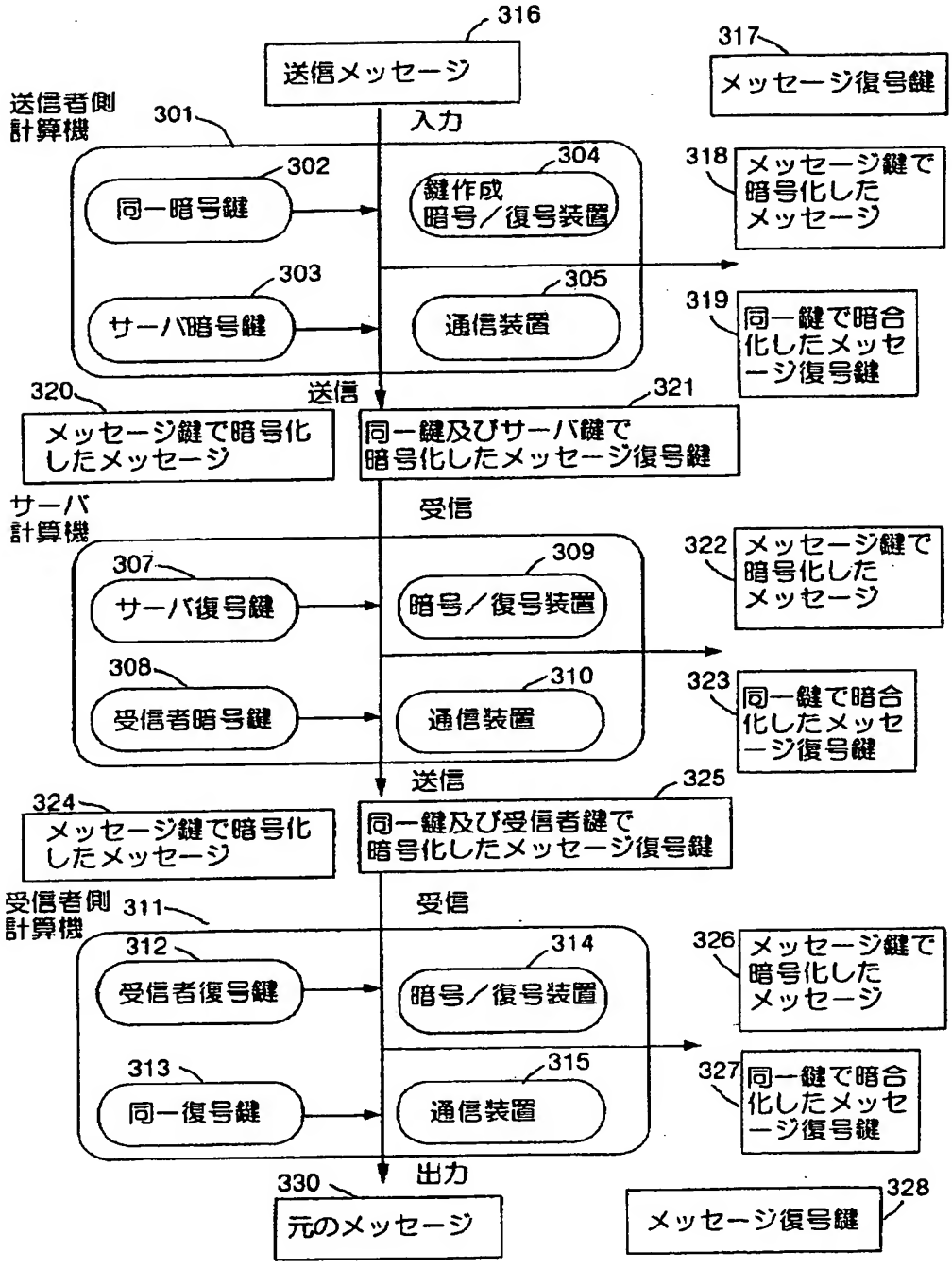
【図２】

図２


送信者側計算機処理
サーバ計算機処理
受信者側計算機処理
201
送信者がメッセージを作成し、送信側の計算機に入力する。
202
送信側計算機が同一暗号鍵でメッセージを暗号化する。
203
送信者側の計算機がサーバ暗号鍵で前記暗号メッセージをさらに暗号化する。
204
送信側の計算機が暗号メッセージをサーバに向け、送信する。
205
サーバ側の計算機が暗号メッセージを受信する。
206
サーバ側の計算機が受信メッセージをサーバの復号鍵で復号する。
207
サーバ側の計算機が前記復号メッセージを受信者の暗号鍵でそれぞれ、暗合する。
208
サーバ側の計算機が受信者に暗号メッセージをそれぞれ、送信する。
209
受信側の計算機が暗号メッセージを受信する。
210
受信者側の計算機が受信メッセージを受信者の復号鍵同一鍵で復号する。
211
受信者側の計算機が前記復号メッセージを同一鍵でさらに復号する。
212
受信者計算機が復号メッセージを出力する。

【図３】

図３


316
送信メッセージ
317
メッセージ復号鍵
送信者側
計算機
301
入力
302
同一暗号鍵
304
鍵作成
暗号／復号装置
318
メッセージ鍵で
暗号化した
メッセージ
303
サーバ暗号鍵
305
通信装置
319
同一鍵で暗合
化したメッセ
ージ復号鍵
320
メッセージ鍵で暗号化
したメッセージ
送信
321
同一鍵及びサーバ鍵で
暗号化したメッセージ復号鍵
サーバ
計算機
受信
307
サーバ復号鍵
309
暗号／復号装置
322
メッセージ鍵で
暗号化した
メッセージ
308
受信者暗号鍵
310
通信装置
323
同一鍵で暗合
化したメッセ
ージ復号鍵
送信
324
メッセージ鍵で暗号化
したメッセージ
325
同一鍵及び受信者鍵で
暗号化したメッセージ復号鍵
受信者側
計算機
311
受信
312
受信者復号鍵
314
暗号／復号装置
326
メッセージ鍵で
暗号化した
メッセージ
313
同一復号鍵
315
通信装置
327
同一鍵で暗合
化したメッセ
ージ復号鍵
出力
330
元のメッセージ
328
メッセージ復号鍵

【図４】

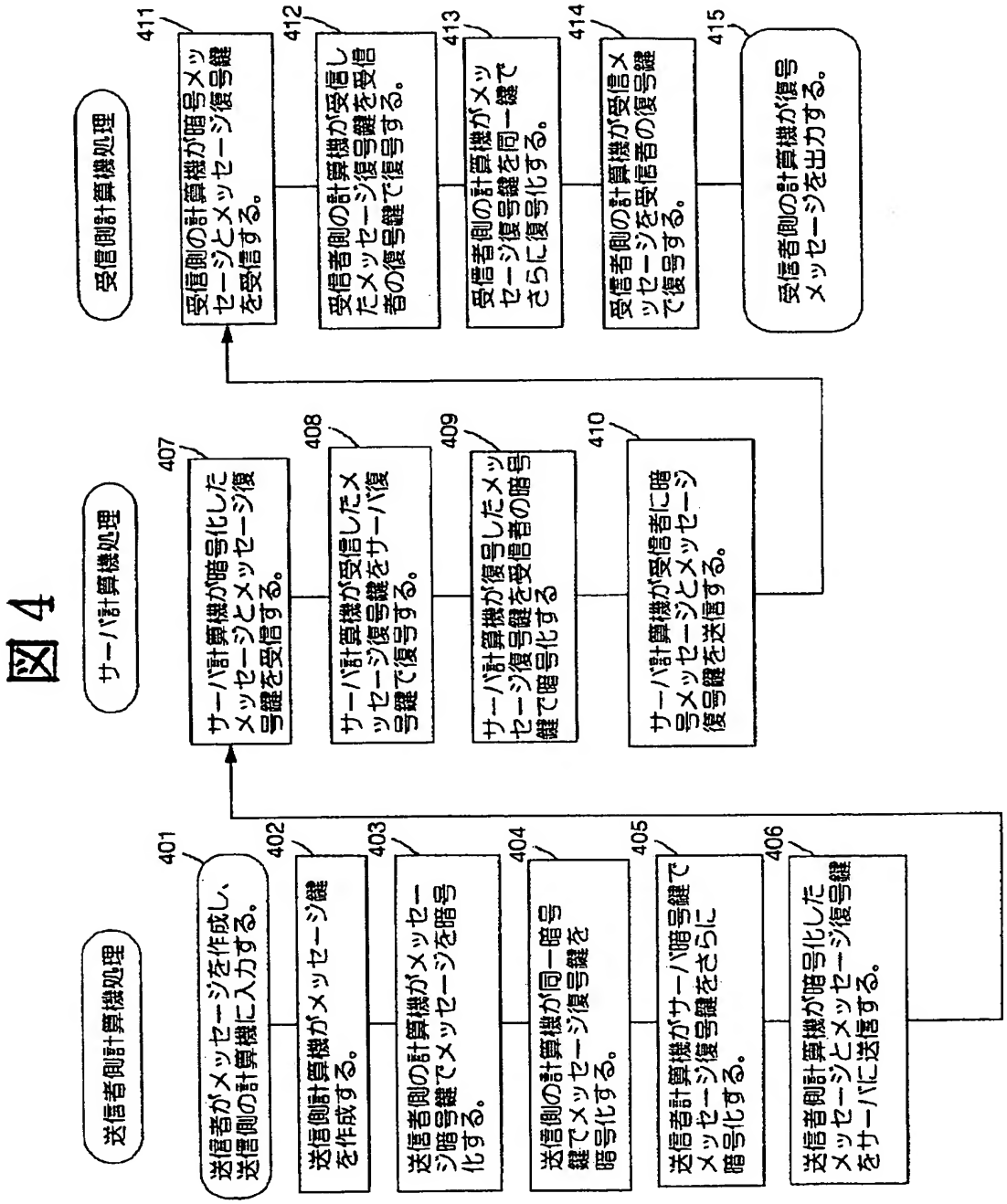


図４

フロントページの続き

(51)Int.Cl.[6]　　識別記号　　ＦＩ

Ｈ０４Ｌ　12/18

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成１１年（１９９９）１１月３０日

【公開番号】特開平１０—１０７８３２
【公開日】平成１０年（１９９８）４月２４日
【年通号数】公開特許公報１０—１０７９
【出願番号】特願平８—２５３５９９
【国際特許分類第６版】
H04L 12/54
12/58
G06F 13/00 351
G09C 1/00 660
H04L 9/14
12/18
【ＦＩ】
H04L 11/20 101 B
G06F 13/00 351 G
G09C 1/00 660 G
H04L 9/00 641
11/18

【手続補正書】
【提出日】平成１１年３月２３日
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】全文
【補正方法】変更
【補正内容】
【書類名】　明細書
【発明の名称】　暗号同報メールシステムの同報通信方法
【特許請求の範囲】
【請求項１】　通信網によって相互接続された複数の送受信者の計算機と同報メール機能を有するメールサーバ計算機からなる同報メールシステムにおいて、
送信者計算機が、メールの受信者計算機が記憶している復号鍵に対応する暗号鍵を用いてメッセージを暗号化した後、前記メールサーバ計算機だけもしくはメールサーバ計算機と送信者計算機のみが記憶している復号鍵に対応する暗号鍵でさらにメッセージを暗号化して、メールサーバ計算機に送信し、メールサーバ計算機は、暗号鍵に対応する復号鍵で一度復号して、受信者計算機に送信することを特徴とする暗号同報メールシステムの同報通信方法。
【請求項２】　請求項１記載の暗号同報メールシステムにおいて、メールサーバ計算機が一度復号した後、受信者計算機だけもしくはメールサーバ計算機と各受信者計算機のみが記憶している復号鍵に対応する暗号鍵でメッセージを暗号化して、各受信者計算機に送信することを特徴とする暗号同報メールシステムの同報通信方法。
【請求項３】　請求項１記載の暗号同報メールシステムにおいて、メールの受信者計算機が記憶している復号鍵に対応する暗号鍵を用いてメッセージを直接暗号化するのではなく、メッセージごとにメッセージ暗号鍵とメッセージ復号鍵を生成し、このメッセージ暗号鍵でメッセージを暗号化し、メッセージ復号鍵をメールの受信者計算機が記憶している復号鍵に対応する暗号鍵を用いて暗号化することを特徴とする暗号同報メールシステムの同報通信方法。
【請求項４】　通信網によって相互接続された複数の送受信者の計算機と同報メール機能を有するメールサーバ計算機からなる同報メールシステムにおいて、
送信者計算機がメールの受信者計算機が記憶している復号鍵に対応する暗号鍵を用いてメッセージ復号鍵を暗号した後、メールサーバ計算機だけもしくはメールサーバ計算機と送信者計算機のみが記憶している復号鍵に対応する暗号鍵でメッセージ復号鍵をさらに暗号化して、暗号化したメッセージとメッセージ復号鍵をメールサーバ計算機に送信し、メールサーバ計算機は、暗号鍵に対応する復号鍵で暗号化したメッセージ復号鍵を一度復号して、暗号化したメッセージとメッセージ復号鍵を受信者計算機に送信することを特徴とする暗号同報メールシステムの同報通信方法。
【請求項５】　請求項４記載の暗号同報メールシステムにおいて、メールサーバ計算機が暗号したメッセージ復号鍵を一度復号した後、受信者計算機だけもしくはメー

ルサーバ計算機と各受信者計算機のみが記憶している復号鍵に対応する暗号鍵でメッセージ復号鍵を暗号して、各受信者計算機に暗号したメッセージとメッセージ復号鍵を送信することを特徴とする暗号同報メールシステムの同報通信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、電子メールシステムにおいて同じ内容のメッセージを複数の人に同報送信する、いわゆる同報メールもしくはメーリングリストサービスに係わる暗号同報メールシステムの同報通信方法に関する。

【０００２】

【従来の技術】メーリングリストで暗号機能を実現するには、従来、３つの方法が知られている。第１の方法は、メーリングリストのメンバに同一の復号鍵を配布し、この復号鍵に対応する暗号鍵を用いてメッセージを暗号化して送信する方法である。

【０００３】第２の方法は、それぞれのメンバが復号鍵を持ち、送信者がそれぞれのメンバ受信者の復号鍵に対応する暗号鍵を用いて暗号化して送る方法である。

【０００４】第３の方法は、それぞれのメンバが復号鍵を持ち、メーリングリストサーバメーリングリスト管理プログラムがそれぞれのメンバの復号鍵に対応する暗号鍵を用いて暗号化して送る方法である。

【０００５】

【発明が解決しようとする課題】前記従来技術には以下のような問題点が挙げられる。

【０００６】前記第１の方法には、メーリングリストメンバが減った場合に問題が起こる。つまり、正規のメンバであった者が、メーリングリストメンバから抜けた後に、ネットワークを盗聴するなどしてメッセージを不法入手し、持っている復号鍵を使って暗号化されたメッセージを復号することができてしまう。これを防ぐためには、メンバが減る度に全てのメンバの鍵を交換する必要がおきてしまい、時間およびコストがかかってしまう。

【０００７】第２の方法では、全ての送信者が全てのメンバの暗号鍵をもっている必要があることに問題がある。例えば、メンバの増減や鍵の交換があると、その度に全ての送信者が自分が保有するメンバの構成を更新したりメンバの鍵を更新する必要があり、第１の方法と同様にコストがかかる。

【０００８】第３の方法では、本来メンバには含まれないメーリングリストサーバが、そして結果的にはサーバの管理者がメッセージ本体にアクセスすることができ、セキュリティ上の問題が生じる。

【０００９】本発明の目的は、これらの問題を解決する暗号同報メールシステムの同報通信方法を提供することである。

【００１０】

【課題を解決するための手段】本発明は、メーリングリストサーバを用い、メッセージを二重に暗号化することで課題を解決する。暗号に用いる鍵として、メンバそれぞれの鍵、メーリングリストサーバの鍵、メンバ共通の同一暗号鍵を用いる。鍵には暗号化に使う鍵と復号に使う鍵の２種類がある。公開鍵暗号方式では、暗号鍵と復号鍵は別の鍵であり、暗号鍵は送信者を含め誰でもアクセスでき公開鍵と呼ばれ、復号鍵は受信者のみアクセスでき個人鍵と呼ばれる。対称鍵暗号方式では、２つの鍵は同一であり秘密鍵と呼ばれることが多い。

【００１１】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態を詳細に説明する。

【００１２】図１は、本発明を適用したシステムの第１の実施形態を示すシステム構成図である。

【００１３】１０１はメーリングリストの参加メンバであり、メーリングリストにメッセージを送る送信者側の計算機（以下、送信者計算機と言う）である。１０２は前記メーリングリストにメッセージを送る送信者計算機１０１が記憶している、メーリングリストの全てのメンバの計算機が持っている同一暗号鍵である。

【００１４】１０３は、送信者計算機１０１が記憶しており、メーリングリストの全てのメンバの計算機が持っているサーバの暗号鍵である。１０４は、送信者計算機１０１が備えており、同一暗号鍵１０２、サーバ暗号鍵１０３を使ってメッセージの暗号化処理や復号処理を行う暗号／復号化処理装置である。１０５は、計算機１０１が備えており、メッセージをネットワークへ送信する通信装置である。

【００１５】１０６はメーリングリストのサーバ計算機である。１０７は、サーバ計算機１０６が記憶し、サーバ暗号鍵１０３に対応するサーバ復号鍵であり、サーバ計算機１０６だけが記憶している。１０８は、サーバ計算機１０６が記憶しており、メンバそれぞれの固有の受信者暗号鍵である。なお、メンバの受信者暗号鍵はメンバの数だけある。

【００１６】１０９はサーバ計算機１０６が備えており、サーバ復号鍵１０７、メンバ固有の受信者暗号鍵１０８を使ってメッセージの暗号化や復号を行う暗号／復号化処理装置である。

【００１７】１１０はサーバ計算機１０６に備えられており、メッセージをネットワークから受信したり、ネットワークへ送信したりする通信装置である。１１１はメーリングリストの参加メンバが使用し、サーバ計算機１０６から送られてきたメッセージを受け取る受信者側の計算機（以下、受信者計算機と言う）である。

【００１８】１１２は受信者計算機１１１が記憶しており、メンバ固有の暗号鍵１１２に対応する受信者復号鍵であり、受信者計算機１１１だけが記憶している。１１２は受信者計算機１１１が記憶しており、メーリングリ

ストの全てのメンバが持っている同一暗号鍵１０２に対応する同一の復号鍵であり、メンバの計算機だけが記憶している。１１４は受信者計算機１１１が備えており、復号鍵１１２、同一復号鍵１１３を使ってメッセージの暗号化や復号を行う暗号／復号化処理装置である。

【００１９】１１５は受信者計算機１１１が備えており、メッセージをネットワークから受信する通信装置である。１１６は送信者が作成するメッセージを示す。１１７は送信者計算機１０１の中で同一暗号鍵１０２と暗号／復号化処理装置１０４を使ってメッセージ１１６を暗号化したメッセージである。

【００２０】１１８はサーバ暗号鍵１０３と暗号／復号化処理装置１０４を使って暗号メッセージ１１７をさらに暗号化したメッセージであり、送信者計算機１０１からサーバ計算機１０６へ通信装置１０５を使いネットワークを経由して送信される。このメッセージ１１８は同一暗号鍵１０２とサーバ暗号鍵１０３を使い、二重に暗号化されている複合暗号メッセージである。

【００２１】１１９はサーバ計算機の中でサーバ復号鍵１０７と暗号／復号化処理装置１０９を使って暗号メッセージ１１８を復号したメッセージであり、暗号メッセージ１１７と同一である。

【００２２】１２０はメンバ固有の受信者暗号鍵１０８と暗号/復号化処理装置１０９を使って、暗号メッセージ１１９をさらに暗号化したメッセージ（すなわち、同一暗号鍵１０２および受信者暗号鍵１０８で暗号化したメッセージ）であり、サーバ計算機１０６から受信者計算機１１１へ通信装置１１０を使い、ネットワークを経由して送信される。

【００２３】１２１は受信者計算機１１１の中で復号鍵１１２と暗号／復号化処理装置１１４を使って暗号メッセージ１２０を復号化したメッセージであり、暗号メッセージ１１７、１１９と同一である。１２２は受信者計算機１１１の中で同一復号鍵１１３と暗号／復号化処理装置１１４を使って暗号メッセージ１２１を復号して出力したメッセージであり、送信メッセージ１１６と同一である。なお、本明細書の実施の形態および、図面において、送信者側計算機１０１と受信者側計算機１１１はそれぞれ、単数で開示しているのは説明上の都合であり、それぞれが複数あっても構わない。

【００２４】以下、図２のフロー図にしたがって、具体的な処理を説明する。

【００２５】ステップ２０１からステップ２０４までは、送信者計算機１０１の処理を示す。ステップ２０５からステップ２０８までは、サーバ計算機１０６の処理を示す。ステップ２０９からステップ２１２までは、受信者計算機１１１の処理を示す。

【００２６】送信者がメーリングリスト宛のメッセージ１１６を作成し送信者計算機１０１に入力する（ステップ２０１）。送信者計算機１０１が同一暗号鍵１０２と暗号／復号化処理装置１０４を用いて、入力されたメッセージ１１６を暗号化し、同一暗号鍵１０２で暗号化したメッセージ１１７を生成する（ステップ２０２）。

【００２７】送信者計算機１０１がサーバ暗号鍵１０３と暗号/復号化処理装置１０４を用いて、暗号メッセージ１１７をさらに暗号化し、同一暗号鍵１０２およびサーバ暗号鍵１０３で暗号化したメッセージ１１８を生成する（ステップ２０３）。送信者計算機１０１が通信装置１０５を用いて、先に生成したメッセージ１１８をサーバ計算機１０６宛にネットワークを経由して送信する（ステップ２０４）。

【００２８】送信者計算機１０１が送信した暗号メッセージ１１８をサーバ計算機１０６が、通信装置１１０を用いて受信する（ステップ２０５）。サーバ計算機１０６がサーバ復号鍵１０７と暗号/復号化処理装置１０９を用いて、受信したメッセージ１１８を復号し、同一暗号鍵１０２で暗号化したメッセージ１１９を復元する（ステップ２０６）。

【００２９】サーバ計算機１０６が、受信者暗号鍵１０８と暗号/復号化処理装置１０９を用いて、同一暗号鍵１０２で暗号化されているメッセージ１１９を受信者暗号鍵１０８によってさらに暗号化し、同一暗号鍵１０２および受信者暗号鍵１０８で暗号化したメッセージ１２０を生成する（ステップ２０７）。

【００３０】このステップ２０７の処理は受信者であるメーリングリストのメンバそれぞれに対して行う。つまり、それぞれの受信者の暗号鍵で暗号化し、各受信者ごとに暗号メッセージ１２０を生成する。

【００３１】サーバ計算機１０６が通信装置１１０を用いて、先に生成したメッセージ１２０を受信者計算機１１１宛にネットワークを経由して、送信する（ステップ２０８）。このステップ２０８の処理もそれぞれの受信者に対して繰り返す。つまり、それぞれの受信者の計算機に対応するメッセージ１２０を送信する。

【００３２】サーバ計算機１０６が送信した暗号メッセージ１２０を受信者計算機１１１が、通信装置１１５を用いて受信する（ステップ２０９）。受信者計算機１１１が受信者復号鍵１１２と暗号/復号化処理装置１１４を用いて、受信したメッセージ１２０を復号し、同一暗号鍵１０２で暗号化されているメッセージ１２１を復元する（ステップ２１０）。

【００３３】受信者計算機１１１が同一復号鍵１１３と暗号/復号化処理装置１１４を用いて、同一暗号鍵１０２で暗号化されているメッセージ１２１を復号する（ステップ２１１）。そして、この復号したメッセージ１２２を受信者に対して、出力する（ステップ２１２）。

【００３４】（実施の形態２）次に、図３、図４を用いて本発明の第２の実施形態を詳細に説明する。

【００３５】図３は全体のシステム構成を示す。図３において、３０１はメーリングリストの参加メンバであ

り、メーリングリストにメッセージを送る送信者の計算機である。３０２は送信者計算機３０１が記憶しており、メーリングリストの全てのメンバの計算機が持っている同一の暗号鍵である。

【００３６】３０３は送信者計算機３０１が記憶しており、メーリングリストの全てのメンバの計算機が持っているサーバ計算機の暗号鍵である。３０４は送信者計算機３０１が備えており、メッセージ鍵の生成及びメッセージ暗号化用の鍵３０２、３０３を使ってメッセージやメッセージ鍵の暗号化や復号を行う鍵作成／暗号／復号装置である。３０５は送信者計算機３０１が備えており、メッセージや暗号化した鍵をネットワークへ送信する装置である。

【００３７】３０６はメーリングリストのサーバ計算機である。３０７はサーバ計算機３０６が記憶しており、サーバ暗号鍵３０３に対応する復号鍵であり、サーバ計算機３０６の計算機だけが記憶している。３０８は、サーバ計算機３０６が記憶しており、メンバそれぞれの受信者暗号鍵である。メンバの受信者暗号鍵３０８はメンバの数だけある。３０９は、サーバ計算機３０６が備えており、サーバ復号鍵３０７、受信者暗号鍵３０８を使ってメッセージやメッセージ鍵の暗号化や復号を行う暗号／復号装置である。３１０は、サーバ計算機３０６が備えており、メッセージや暗号化した鍵をネットワークから受信したり、ネットワークへ送信する装置である。

【００３８】３１１はメーリングリストの参加メンバであり、サーバ計算機３０６から送られてきたメッセージを受け取る受信者の計算機である。３１２は受信者計算機３１１が記憶しており、受信者暗号鍵３０８に対応する受信者復号鍵であり、受信者計算機３１１だけが記憶している。

【００３９】３１３は、受信者計算機３１１が記憶しており、メーリングリストの全てのメンバが持っている同一暗号鍵３０２に対応する同一の復号鍵であり、メンバの計算機だけが記憶している。

【００４０】３１４は受信者計算機３１１が備えており、受信者復号鍵３１２、同一復号鍵３１３を使ってメッセージやメッセージ鍵の暗号化や復号を行う暗号／復号装置である。

【００４１】３１５は、受信者計算機３１１が備えており、メッセージや暗号化した鍵をネットワークから受信する通信装置である。３１６は送信者が作成するメッセージを示す。３１７は鍵作成／暗号／復号装置３０４が生成したメッセージ鍵である。

【００４２】３１８は送信者計算機３０１の中で鍵作成／暗号／復号装置３０４が生成したメッセージ鍵３１７と、鍵作成／暗号／復号装置３０４を使って送信メッセージ３１６を暗号化したメッセージである。３１９は同一暗号鍵３０２と鍵作成／暗号／復号装置３０４を使ってメッセージ鍵３１７を暗号化したメッセージ鍵である。

【００４３】３２０は暗号メッセージ３１８と同一であり、送信者計算機３０１からサーバ計算機３０６へ通信装置３０５を使い、ネットワークを経由して送信される。３２１はサーバ暗号鍵３０３と鍵作成／暗号／復号装置３０４を使って、メッセージ鍵３１９を暗号化したメッセージ鍵（すなわち、メッセージ鍵３１７を同一暗号鍵３０２で暗号化し、さらにサーバ暗号鍵３０３で暗号化した鍵）であり、送信者計算機３０１からサーバ計算機３０６へ通信装置３０５を使い、ネットワークを経由して送信される。

【００４４】メッセージ鍵３２１は同一暗号鍵３０２とサーバ暗号鍵３０３の鍵を使い、二重に暗号化されている。暗号化メッセージ３２２は暗号化メッセージ３１８、３２０と同一であり、受信した暗号メッセージである。３２３はサーバ計算機３０６の中でサーバ復号鍵３０７と暗号／復号装置３０９を使って、メッセージ鍵３２１を復号したメッセージ鍵（すなわち、同一暗号鍵３０２で暗号化したメッセージ鍵）である。

【００４５】３２４は暗号化メッセージ３１８、３２０、３２２と同一であり、サーバ計算機３０６から受信者計算機３１１に対し通信装置３１０を使い、ネットワークを経由して送信される。

【００４６】３２５は受信者暗号鍵３０８と暗号／復号装置３０９を使って、同一暗号鍵３０２で暗号化したメッセージ鍵３２３を受信者暗号鍵３０８によってさらに暗号化したメッセージ鍵であり、サーバ計算機３０６から受信者計算機３１１へ通信装置３１０を使い、ネットワークを経由して送信される。

【００４７】３２６は暗号化メッセージ３１８、３２０、３２２、３２４と同一であり、受信した暗号メッセージである。３２７は受信者計算機３１１の中で受信者復号鍵３１２と暗号／復号装置３１４を使ってメッセージ鍵（同一暗号鍵と受信者暗号鍵で暗号化した鍵）３２５を復号したメッセージ鍵である。

【００４８】３２８は同一復号鍵３１３と暗号／復号装置３１４を使って、同一暗号鍵で暗号化したメッセージ鍵３２７を同一復号鍵３１３で復号したメッセージ鍵で、メッセージ鍵３１７と同一である。

【００４９】３３０はサーバ計算機３０６の中でメッセージ復号鍵３２８と暗号／復号装置３１４を使って、メッセージ鍵で暗号化したメッセージ３２６を復号し、出力したメッセージで、送信メッセージ３１６と同一である。

【００５０】以下、図４のフロー図にしたがって、処理を説明する。

【００５１】ステップ４０１から４０６までは、送信者計算機３０１の処理を示す。ステップ４０７から４１０までは、サーバ計算機３０６の処理を示す。ステップ４１１から４１５までは、受信者計算機３１１の処理を示

す。

【００５２】送信者がメーリングリスト宛のメッセージ３１６を作成し、送信者計算機３０１に入力する（ステップ４０１）。送信者計算機３０１が鍵生成／暗号／復号装置３０４を使ってメッセージ鍵３１７を生成する（ステップ４０２）。

【００５３】送信者計算機３０１が先に生成したメッセージ鍵３１７と鍵生成／暗号／復号装置３０４を用いて、入力された送信メッセージ３１６をメッセージ鍵３１７で暗号化し、メッセージ鍵３１７で暗号化したメッセージ３１８を生成する（ステップ４０３）。

【００５４】送信者計算機３０１が同一暗号鍵３０２と鍵作成／暗号／復号装置３０４を用いて、メッセージ鍵３１７を暗号化し、同一暗号鍵３０２で暗号化したメッセージ鍵３１９を生成する（ステップ４０４）。

【００５５】送信者計算機３０１がサーバ暗号鍵３０３と鍵作成／暗号／復号装置３０４を用いて、同一暗号鍵３０２で暗号化したメッセージ鍵３１９をサーバ暗号鍵３０３でさらに暗号化し、同一暗号鍵３０２およびサーバ暗号鍵３０３で暗号化したメッセージ鍵３２１を生成する（ステップ４０５）。

【００５６】送信者計算機３０１が通信装置３０５を用いて、先に暗号化したメッセージ３１８と同一のメッセージ３２０と同一暗号鍵３０２およびサーバ暗号鍵３０３で暗号化したメッセージ鍵３２１をサーバ計算機３０６宛にネットワークを経由して送信する（ステップ４０６）。

【００５７】送信者計算機３０１が送信したメッセージ３２０とメッセージ鍵３２１をサーバ計算機３０６が通信装置３１０を用いて、受信する（ステップ４０７）。

【００５８】サーバ計算機３０６がサーバ復号鍵３０７と暗号／復号装置３０９を用いて、受信したメッセージ鍵３２１を復号し、同一暗号鍵３０２で暗号化されているメッセージ鍵３２３を復元する（ステップ４０８）。この時、暗号化したメッセージ３２２はそのままである。

【００５９】サーバ計算機３０６が、受信者暗号鍵３０８と暗号／復号装置３０９を用いて同一暗号鍵３０２で暗号化したメッセージ鍵３２３を暗号化し、同一暗号鍵３０２および受信者暗号鍵３０８で暗号化したメッセージ鍵３２５を生成する（ステップ４０９）。このステップ４０９の処理は、受信者であるメーリングリストのメンバそれぞれに対して行う。つまり、それぞれの受信者の暗号鍵で暗号化し、各受信者ごとに暗号したメッセージ鍵３２５を生成する。

【００６０】サーバ計算機３０６が通信装置３１０を用いて、先に生成したメッセージ鍵３２５と暗号化したメッセージ（３２２と同一）３２４を受信者計算機３１１宛にネットワークを経由して送信する（ステップ４１０）。このステップ４１０の処理もそれぞれの受信者に対して繰り返す。つまり、それぞれの受信者の計算機に暗号したメッセージ３２４と受信者に対応するメッセージ鍵３２５を送信する。

【００６１】サーバ計算機３０６が送信した暗号化されたメッセージ３２４とメッセージ鍵３２５を受信者計算機３１１が通信装置３１５を用いて受信する（ステップ４１１）。

【００６２】受信者計算機３１１が受信者復号鍵３１２と暗号／復号装置３１４を用いて、受信したメッセージ鍵３２５を復号し、同一暗号鍵３０２で暗号化されているメッセージ鍵３２７を復元する（ステップ４１２）。この時、暗号化されているメッセージ３２６はそのままである。

【００６３】受信者計算機３１１が受信者復号鍵３１２と暗号／復号装置３１４を用いて、同一暗号鍵３０２で暗号化されているメッセージ鍵３２７を復号し、元のメッセージ鍵３１７と同じメッセージ鍵３２８を得る（ステップ４１３）。暗号化されているメッセージ３２６をメッセージ鍵３２８と暗号／復号装置３１４を用いて復号する（ステップ４１４）。この復号したメッセージ３３０を受信者に対して出力する（ステップ４１５）。なお、本発明では、メッセージ鍵と復号鍵とを別物として説明したが、秘密鍵暗号を用いてメッセージを暗号化する場合には、同一の鍵となる。

【００６４】

【発明の効果】本発明によると、送信者からサーバに送られるメッセージもしくはメッセージ鍵は、メンバが共通に持っている鍵で暗号され、さらにサーバの鍵で暗号されているので、サーバだけが復号できる。

【００６５】また、メーリングリストから抜けてしまったメンバはたとえ、メンバ同一の復号鍵を持っていてもアクセスできない。メンバが減った時には、メールサーバ計算機内部の変更だけで済み、メンバ送受信者の計算機の変更が不要になる。

【００６６】また、メッセージもしくはメッセージ鍵はメンバ計算機だけが復号できる同一鍵で暗号されているのでメールサーバ計算機はアクセスすることができず、第３者による盗聴、情報の漏洩を防ぐことができる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態を示すシステム構成図である。

【図２】本発明の第１の実施の形態の処理を示すフローチャートである。

【図３】本発明の第２の実施形態を示すシステム構成図である。

【図４】本発明の第２の実施の形態の処理を示すフローチャートである。

【符号の説明】

１０２…同一暗号鍵、１０３…サーバ暗号鍵、１０４，１０９，１１４…暗号/復号化処理装置、１０５，１１

０，１１５…通信装置、１０７…サーバ復号鍵、１０８…受信者暗号鍵、１１２…受信者復号鍵、１１３…同一復号鍵。

【手続補正２】

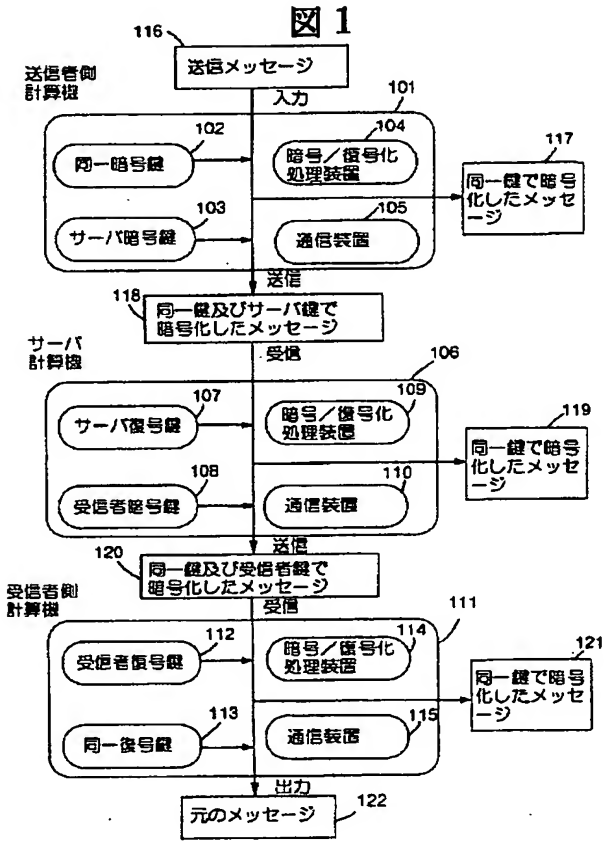
【補正対象書類名】図面

【補正対象項目名】全図

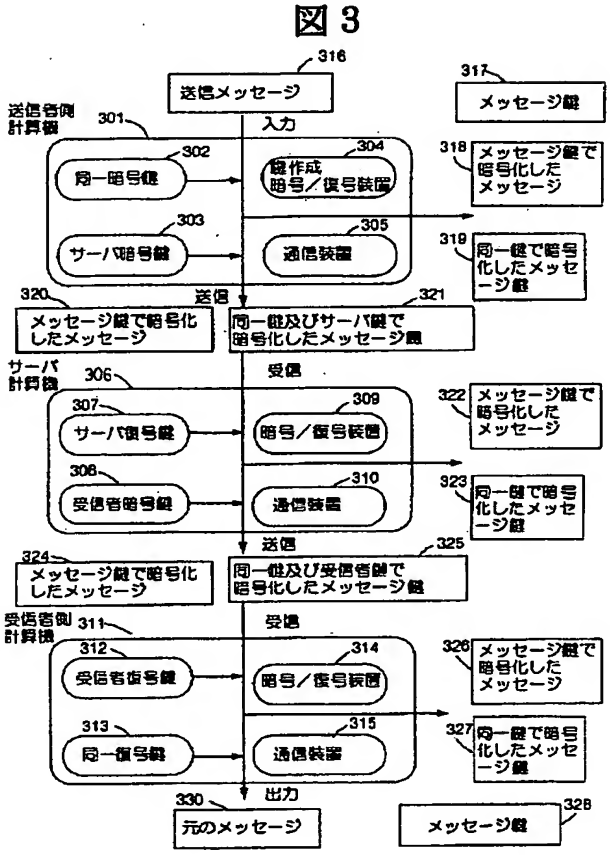
【補正方法】変更

【補正内容】

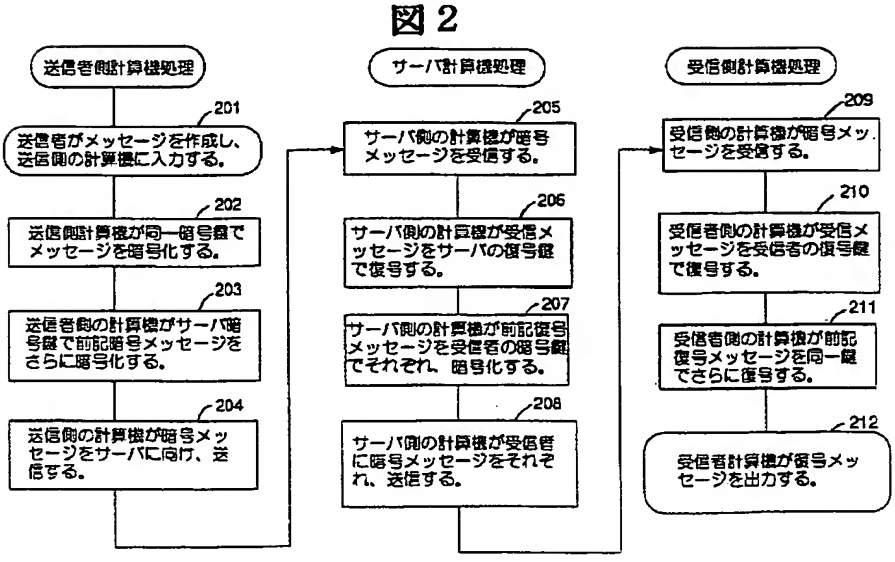
【図１】



【図３】

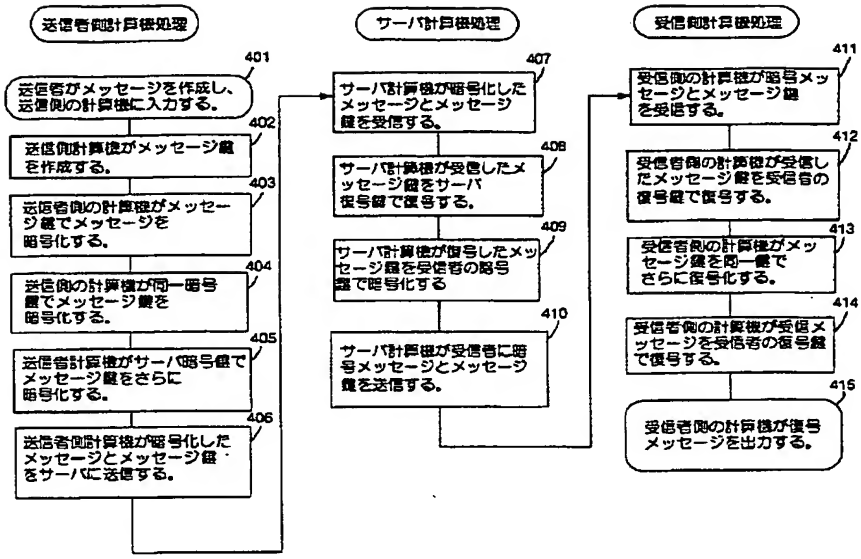


【図２】



【図４】

図４


送信者側計算機処理
サーバ計算機処理
受信側計算機処理
401
送信者がメッセージを作成し、送信側の計算機に入力する。
402
送信側計算機がメッセージ鍵を作成する。
403
送信者側の計算機がメッセージ鍵でメッセージを暗号化する。
404
送信側の計算機が同一暗号鍵でメッセージ鍵を暗号化する。
405
送信者計算機がサーバ暗号鍵でメッセージ鍵をさらに暗号化する。
406
送信者側計算機が暗号化したメッセージとメッセージ鍵をサーバに送信する。
407
サーバ計算機が暗号化したメッセージとメッセージ鍵を受信する。
408
サーバ計算機が受信したメッセージ鍵をサーバ復号鍵で復号する。
409
サーバ計算機が復号したメッセージ鍵を受信者の暗号鍵で暗号化する
410
サーバ計算機が受信者に暗号メッセージとメッセージ鍵を送信する。
411
受信側の計算機が暗号メッセージとメッセージ鍵を受信する。
412
受信者側の計算機が受信したメッセージ鍵を受信者の復号鍵で復号する。
413
受信者側の計算機がメッセージ鍵を同一鍵でさらに復号化する。
414
受信者側の計算機が受信メッセージを受信者の復号鍵で復号する。
415
受信者側の計算機が復号メッセージを出力する。